PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00 — A1

(11) International Publication Number: WO 95/14265

(43) International Publication Date: 26 May 1995 (26.05.95)

(21) International Application Number: PCT/GB94/02508

(22) International Filing Date: 14 November 1994 (14.11.94)

(30) Priority Data:
9323453.2 13 November 1993 (13.11.93) GB

(71) Applicant *(for all designated States except US)*: CALLUNA TECHNOLOGY LIMITED [GB/GB]; Level 2, Saltire Court, 20 Castle Terrace, Edinburgh EH1 2ET (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: STEWART, Alec, Donald [GB/GB]; 11 Bankfoot Park, Scotlandwell, Kinross KY13 7JP (GB). MATHERS, Stewart [GB/GB]; 12 Ashgrove Street, Ayr, Scotland (GB).

(74) Agents: McCALLUM, William, Potter et al.; Cruikshank & Fairweather, 19 Royal Exchange Square, Glasgow G1 3AE (GB).

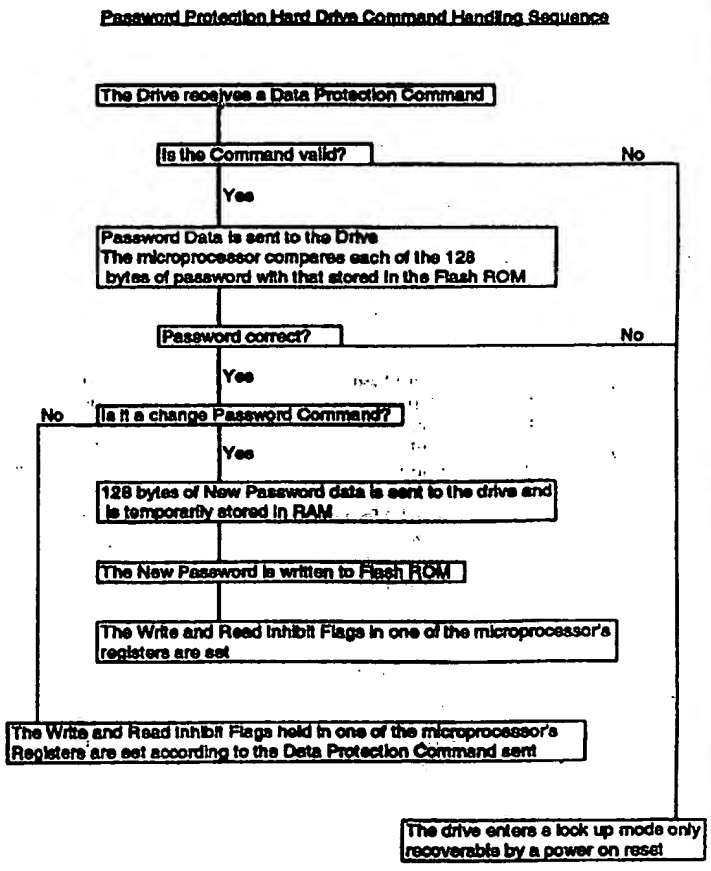
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ).

Published
With international search report.

(54) Title: SECURITY SYSTEM FOR HARD DISK DRIVE

(57) Abstract

A portable hard disk drive has an electrically erasable programmable read-only-memory (EEPROM) for storing a first password for allowing a user access to the disk and a random access memory (RAM) for temporarily storing a password entered by a user. A microprocessor is arranged to compare the user-entered password passed with the password stored in the EEPROM and to generate a signal to allow a user access to the disk if a valid match is found and to prohibit access if there is no match.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

Security system for hard disk drive

The present invention relates to a security system intended for the protection of information recorded on miniature portable hard disk drives for use typically in small portable computers.

The advent of the PCMCIA interface and accompanying plug-compatible memory products means that truly portable mass storage devices will soon become commonplace and easily interchangeable between computer systems and similar devices.

The need for protection of confidential data files is of prime importance in these small disk drives as they can easily be lost or stolen and thus become available to unauthorised users. A method of protection and the protection apparatus must exist in the drive itself to ensure that it is secure wherever it is plugged in and run.

Current methods of file protection such as those included within application software or those using separate utility software packages are not particularly suited to portable devices as they can either be easily decoded by someone skilled in the art or form part of the host system memory.

A first object of the present invention is to provide a method of securing the files on a hard disk drive by means of user password protection.

A second object of the present invention is to provide a system and method of securing the files on a hard disk drive for "read only" operation.

A third object of the present invention is to provide a method of securing the files on a hard disk drive such that "no access" is permitted.

A fourth object of the present invention is to provide a method of providing a Master Key password for authorised secondary access in the event that the user password is lost.

A fifth object of the present invention is to provide a method of protecting the password from discovery by

enciphering software programs.

A sixth object of the invention is to provide a system and apparatus to enable the method to be implemented.

In accordance with the present invention there is provided a memory and comparison means with a special utility program to enable the owner or user of a hard disk drive to protect the data files by setting an access password.

According to a first aspect of the present invention there is provided a security system for a portable hard disk drive, said system comprising:

first memory means for storing a password for allowing a user to have access to information on the disk;

second memory means for storing a user-entered password; and

comparison means coupled to said first memory means and to said second memory means for comparing the stored password with the user-entered password and for permitting access to information on the disk if the passwords match and preventing access when there is no match.

The password is conveniently stored in flash or other solid state non-volatile memory on the disk drive electronics board and it controls unauthorised access of the drive depending on the level of protection selected. Code used to interact with an utility program which is run on a computer in which the disk drive is being used in order to provide a reasonably user-friendly interface for entry and/or amendment of passwords, setting of protection mode etc, is also conveniently stored in flash or other solid state memory (which may be the same device as that in which the password is stored), on the disk drive electronics board, so that the main part of the security system is largely contained in the portable disk drive itself. In one possible form of the invention though the utility software may be formed and arranged to read in a computer system identification number (e.g. the BIOS Serial No) and use this as a "user input" password to be compared against a stored password so that the drive is

"protected" for automatic access only (possibly subject to use of a master password) from a particular computer.

The user may advantageously have the option of setting two or more different levels of security required, such as "no protection", "read only" or "full protection".

In "no protection" mode the drive password defaults to a free access condition. In "read only" mode, files can be read but not altered and new files may not be added to the drive. In "no access" mode the drive will not allow any access.

A Master Password is desirably provided which is stored in a different location in the flash memory. This can only be used by suitable authorised personnel to over-ride any user selected password, for example in the event of a regular password being forgotten. The Master Password could be set during the manufacture of the drive, but more conveniently is set by a purchaser of the disk drive.

The system advantageously has means which prevent the use of special computer programs to decode the password and thereby gain access to the protected files so that if an illegal password is attempted, the drive "hangs" and requires a power-on reset before the password can be re-entered.

Preferably, said first memory means is a non-volatile read-only-memory (ROM). Where a volatile memory is used then the system should of course be provided with power supply means or at least back-up power supply means, though this is generally less convenient. Preferably, said second memory means is a random access memory.

Conveniently, said comparison means is a microprocessor which is formed and arranged to fetch a code corresponding to said stored password from the first memory, fetch a code corresponding to the "user-entered" password, and store the codes in first and second registers, and then compare the contents of the registers and only if there is a valid match, access to the disk drive is permitted. Advantageously the microprocessor is further formed and arranged so that if there is no valid

match then the drive "hangs" and requires a power-on reset before a new password is entered.

The first memory (e.g. non-volatile ROM), second memory (e.g. random access memory) and comparison means (e.g. microprocessor) are all conveniently provided in solid state device means on a printed circuit board used for controlling the disk drive (e.g. a PCMCIA Type III hard disk drive).

According to a second aspect of the present invention, there is provided a method of controlling access to a portable hard disk drive comprising the steps of:

storing a first password in a first, usually non-volatile memory;

storing a user-entered password in a second memory;

comparing the first password with the user-entered password; and

if a valid match is found, allowing the user access to the disk drive.

Preferably, the method includes the step of allowing the user selectively to access one of a plurality of different protection levels by entering a code corresponding to the protection level together with the password.

Preferably also, the method includes the step of altering the password stored in the non-volatile memory by entering a code corresponding to a password change, together with the existing password stored in said volatile memory and the new password to be stored, so that said new password replaces said existing password.

Conveniently, said codes corresponding to different levels of data protection and said passwords are entered from a keyboard of a computer in which the disk drive has been installed via a software utility run on that computer.

According to another aspect of the present invention, there is provided a circuit board for use with a portable disk drive for controlling access to information on the disk, said circuit board comprising disk drive control

means for controlling the rotation of the disk and for writing and reading information to and from the disk, first memory means disposed on said circuit board for storing first password for allowing a user access to the disk, second memory means disposed on the circuit board for storing a password entered by a user, comparison means mounted on the circuit board and coupled to the first and to the second memory means for comparing the stored first password with the user-entered password and for generating an access control signal to allow the user access to the disk if a valid match is found and to prohibit access if there is no match.

These and other aspects of the invention will become apparent from the following description when taken in combination with the accompanying drawings in which:-

Figs. 1 and 2 are top and bottom views of a PCB layout for a PCMCIA type III disk drive;

Fig. 3 is a circuit block diagram representing the electronic circuitry shown in Figs. 1 and 2

Fig. 4 is a flowchart of the sequence of operation which takes place when a user requires to set a hard disk into 'No Data Protection Mode'; and

Fig. 5 is a flowchart of the sequence of operations which takes place when the disk drive receives a 'Data Protection Command'.

Reference is first made to Figs. 1 and 2 of the drawings which depict a printed circuit board generally indicated by reference numeral 10 which has a plurality of electronic components (IC2-IC9) thereon, as indicated in Fig. 1, and which has a central aperture 12 for receiving the protruding flange of a spindle motor (not shown in the interests of clarity).

The general principles of operation of a PCMCIA disk drive are well known and will not be discussed further, as these are disclosed in applicants' copending U.K. Application No. 9224176.9 and corresponding patent publication No. WO94/11877. As can be seen from Figs. 1, 2 and 3, IC5 is a non-volatile flash EPROM (e.g. ATMEL AT29C512 (64K bytes) in a 32 pin TSOP package)

constituting a first memory means. A user-defined password is stored in IC5. A software utility is run on the computer for setting the password and subsequent entry and/or editing of the password for access to the drive data. The user's password is stored in IC7 STATIC RAM (e.g. Sony CXK5827ATM (32K bytes) in a 28 pin TSOP package).

The code for interacting with the software utility is also stored in the flash EEPROM IC5 and is read into the DSP RAM in the disk drive microprocessor IC4 (preferably a Zilog 286C95 in 100 pin VQFP package) prior to rewriting a new password in the DSP RAM.

As described above there are various levels of data protection which can be implemented with this system. A vendor unique interface command 82h is used to control the data protection mechanism in the drive. This is transparent to the user: it is not menu driven, and software recognises the input code (a to c) to determine the level of protection required. Five different levels of protection are provided as follows:-

a) No data protection (write and read access permitted);

b) Partial data protection (read access only permitted);

c) Full data protection (no data access permitted);

d) Low-level password alteration; and

e) Master key password alteration.

It will be appreciated that the passwords are entered from the keyboard of a computer in which the disk drive has been installed, via a menu-driven utility. The low-level and master key passwords each consist of a 127 bytes of data (the 128th byte being conveniently used to set a flag indicating current access mode whereby this can be "remembered" by the system for a subsequent access). The low-level password default is all 'FFh's which serves as the only means of permanently disabling the drive's Data Protection system. Master key Password support is also provided as a means for over-riding the Low-Level Password.

Once a valid Low-Level Password has been set (i.e. at least one of its 127 bytes is non FFh) the drive will default on a subsequent power up to Full Data Protection Mode.

In one embodiment of the invention each of the three Data Protection modes is volatile and only remain in operation until the drive is powered off and a re-powering up returns the drive to the Full Data Protection Mode. In a preferred embodiment though, as noted above, re-powering up can be arranged to restore the protection mode last set. This is particularly useful where for example it is desired to provide read-only access to one or more users who are not password holders to allow such users readily to access data whilst preventing any unauthorized tampering with the data - for example, where portable hard disk drives are used to supply spare part, product and/or pricing data which requires to be updated more or less frequently, to service centres, supermarkets or the like which use computerized files, manufacturers etc.

The particular protection levels are as follows:-

a) No Data Protection Mode

This function allows the drive to operate in a mode where both Write and Read operations are permissible. It is executed internally under the control of the microprocessor IC4 via the following sequence :-

Set the Sector Count Register to	93h	
Set the Sector Number Register to	42h	
Set the Cylinder Low Register to	69h	
Set the Cylinder High Register to	26h	
Set the Drive/Head Register to	00h	(No data protection function)
Set the Command Register to	82h	(Data protection command)

Wait until the Status Register has Busy (Bit 7) = 0 and DRQ (Bit 3) = 1 Password loop:

Wait until the Drive/Head Register Bits 0-3 = Fh
Set the Sector Count Register with the first (or next) Password byte
Set the Drive/Head Register to 00h
Repeat Password loop until all 127 bytes of the Password have been transferred.
Wait for the Status Register DRQ (Bit3) = 0

An Interrupt shall also be generated by the drive upon command completion.

Read and Write Data access of the drive shall now be permitted. The above is best seen with reference to the flowchart in Figs. 4 and 5 of the drawings. Similar flowcharts are used for protection levels b) and c) and the flowchart in Fig. 5 is also applicable to password changing as will be described.

b) Partial Data Protection Mode

This function is implemented in exactly the same way as that of the No Data Protection Mode with the exception of the Drive/Head Register being set to 01h prior to setting the Command Register.

Once the command is completed, Read Data access only shall be permitted. Attempts at sending write commands shall result in Aborted Command Errors.

c) Full Data Protection Mode

This function is implemented in exactly the same way as that of the No Data Protection Mode with the exception of the Drive/Head Register being set to 02h prior to setting the Command Register.

Once the command is completed, No Data access shall be permitted. Attempts at sending Write or Read commands shall result in Aborted Command Errors.

d) Low-Level Password Alteration

The Low-Level Data Protection Password can be changed by sending the old Low-Level Password along with the new one in the following command sequence:-

Set the Sector Count Register to 93h
Set the Sector Number Register to 42h
Set the Cylinder Low Register to 69h
Set the Cylinder High Register to 26h

Set the Drive/Head Register to 03h
(Password Alteration Function)
Set the Command Register to 82h
(Data Protection Command)

Wait until the Status Register has Busy (bit 7) = 0 and DRQ (bit 3) = 1
Password_loop_1:
Wait until the Drive/Head Register Bits 0-3 = Fh
Set the Sector Count Register with the first (or next) Old Password byte
Set the Drive/Head Register to 00h
Repeat Password_loop_1 until all 128 bytes of the Old Password have been transferred.
Wait for the Status Register DRQ (bit 3) = 0
Password_loop_2:
Wait until the Drive/Head Register Bits 0-3 = Fh
Set the Sector Count Register with the first (or next) New Password byte
Set the Drive/Head Register to 00h
Repeat Password_loop_2 until all 127 bytes of the Old Password have been transferred.
Wait until the Sector Count Register = 01h.
An Interrupt shall also be generated by the drive upon command completion.

e) Master Key Password Alteration

The Master Key Protection Password can be changed by sending the old Master Key Password along with the new one in a sequence identical to that of altering the Low-Level Password with the exception of setting the Drive/Head Register to 04h prior to writing the Command Register.

The setting of a new Master Key Password ordinarily has no effect on the existing Low-Level Password. However, knowledge and unplementatin of the Master Key Password allows a user to change a Low-Level Password. This provides a means for recovering a drive whereby data protection has been invoked but the password has been forgotten. The intention of implementing the Master Key option is for use by restricted personnel only.

Any incorrect attempt at executing a Data Protection Command Function shall result in the drive being disabled where only a power-on reset shall re-enable the interface. This prevents the use of a systematic 'Guess-the-Password-Utility' being used which sends an incrementing password to the drive until it gets it correct.

It will be understood that various modifications may be made to the invention hereinbefore described without departing from the scope of the invention. For example, one or more of the memory chips may be combined with the microprocessor in a single chip instead of separate chips as disclosed in the embodiment. The system is applicable to all sizes of portable hard disk drive, not necessarily PCMCIA type interfaces.

A principal advantage of the invention is that the security system is actually present in the disk drive itself. This means that both the hardware and software is present so that if the disk drive is moved between different machines, the security system will remain in place. A further advantage is that the security system is readily implemented on the disk drive PCB using the existing chip already necessary to control the operation of the disk drive. In addition, the control software is readily loaded into the disk drive circuit.

A further advantage is that various levels of protection can be readily set and passwords can be updated to reflect a variety of changing circumstances.

CLAIMS

1. A security system for a portable hard disk drive, the system comprising:

first memory means for storing a first password for allowing a user to have access to information on the disk drive;

second memory means for storing a second user-entered, password; and

comparison means coupled to the first memory means and to the second memory means for comparing the first and second passwords and for permitting access to information on the disk if the passwords match and preventing access when there is no match.

2. A circuit board for use for with a portable disk drive for controlling access to information on the drive, the circuit board comprising disk drive control means for controlling rotation of the disk and for writing and reading information to and from the disk; first memory means disposed on the circuit board for storing a first password for allowing a user access to the disk; second memory means disposed on the circuit board for storing a second password entered by a user, comparison means mounted on the circuit board and coupled to the first and to the second memory means for comparing the first and second passwords and for generating a signal to allow the user access to the disk if a valid match is found and to prohibit access if there is no match.

3. A system according to claim 1 or a circuit board according to claim 2, wherein the first memory means is a non-volatile read-only-memory (ROM).

4. A system or circuit board according to claim 3, wherein the read-only-memory is an electrically eraseable programmable read-only-memory (EEPROM).

5. A system or a circuit board according to claim 4, wherein a voltage is used an EEPROM which EEPROM requires to both write data to and erase data from the EEPROM which voltage is in the range from 4.5 to 5.5 volts so that data can be erased from the EEPROM by a microcontroller.

6. A system according to claim 1 or to any one of claims

3 to 5 or a circuit board according to any one of claims 2 to 5, wherein the second memory means is random access memory (RAM).

7. A system according to claim 1 or to any one of claims 3 to 6 or a circuit board according to any one of claims 2 to 6, wherein the comparison means is a microprocessor arranged to fetch a code corresponding to said first password from the first memory means and to fetch a code corresponding to the user-entered password from the second memory means and to store these codes in first and second registers prior tocarrying out said comparison.

8. A system according to claim 1 or to any one of claims 3 to 7 or a circuit board according to any one of claims 2 to 7 which includes means for disabling the portable disk drive in the event that the user-entered password does not match the first password so that a power-on reset is required before a new password can be entered by the user.

9. A system according to claim 1 or to any one of claims 3 to 8 or a circuit board according to any one of claims 3 to 8, wherein the first memory means is arranged to store at least a part of a software code for controlling the comparison means.

10. A system according to claim 1 or to any one of claims 3 to 9 or a circuit board according to any one of claims 2 to 9, wherein the first memory means is arranged to store at least two passwords each of which each provides a user with a different level of access.

11. A system or a circuit board according to claim 10, wherein the comparison means is arranged to recognise when a user-entered password is a high-level password and to subsequently enable the user to define the level of access which is obtained by a user entering a low-level password.

12. A system or a circuit board according to claim 11, wherein the levels of access which can be set to include a no-data protection mode in which data can be freely written to and read from the disk drive, and a partial data protection mode in which data can only be read from the disk drive.

13. A method of controlling access to a portable hard

disk drive and comprising the steps of:

storing a first password in a non-volatile memory;

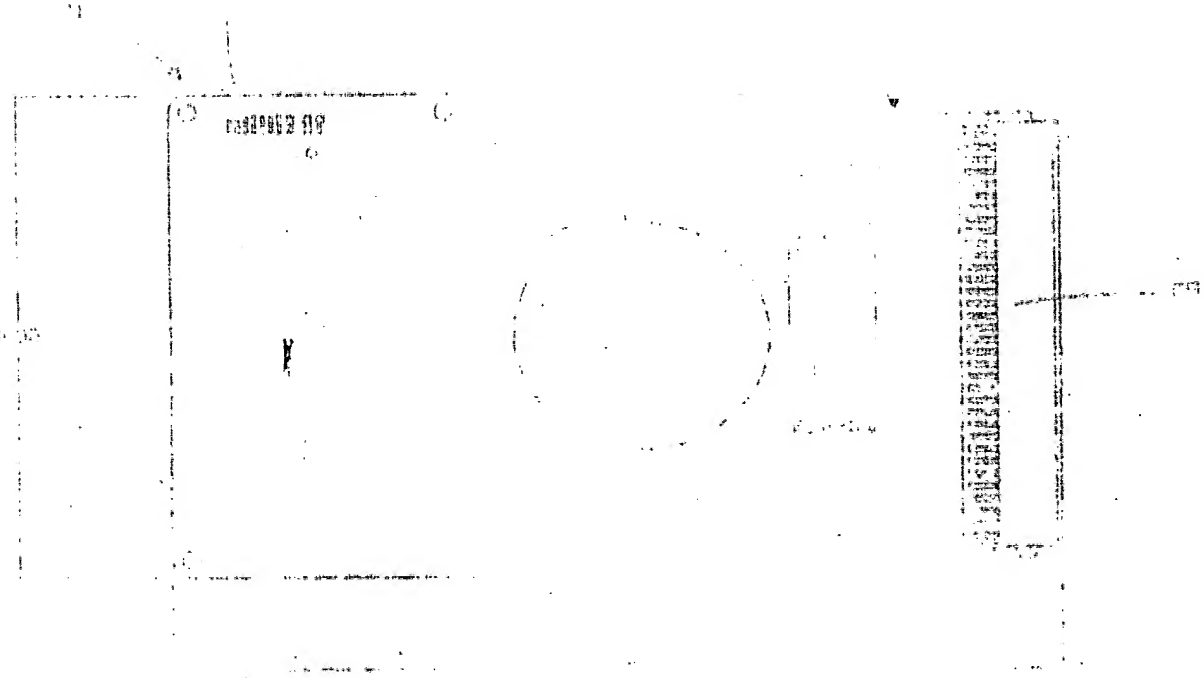
storing a second, user-entered, password in a second memory;

comparing the first and second passwords; and

if a valid match in found, allowing the user access to the disk drive.

14. A method according to claim 13 and including the step of allowing a user access to one of a plurality of different protection levels by entering a code corresponding to the protection level, together with the password.

15. A method according to claim 13 or claim 14 and including the step of altering the password stored in the non-volatile memory by entering a code corresponding to a password change, together with the existing password stored in the volatile memory and the new password to be stored, whereby the new password replaces the existing password.



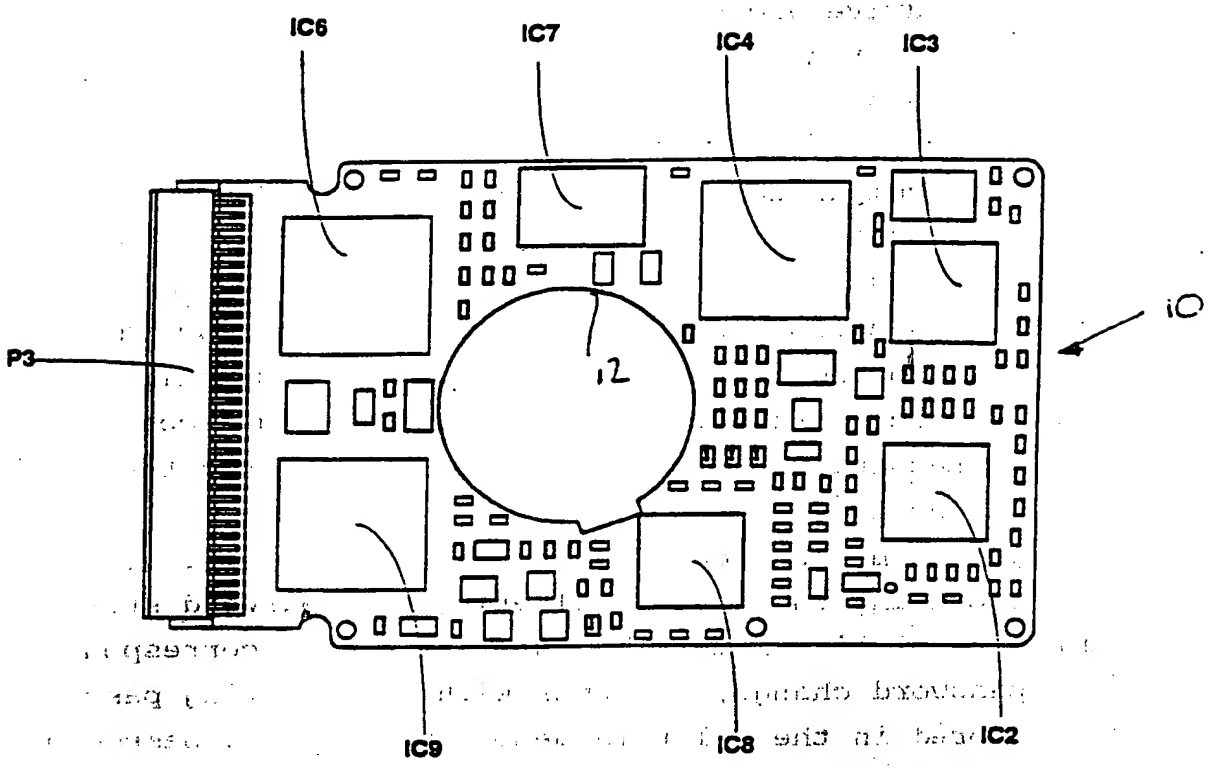


FIG. 1

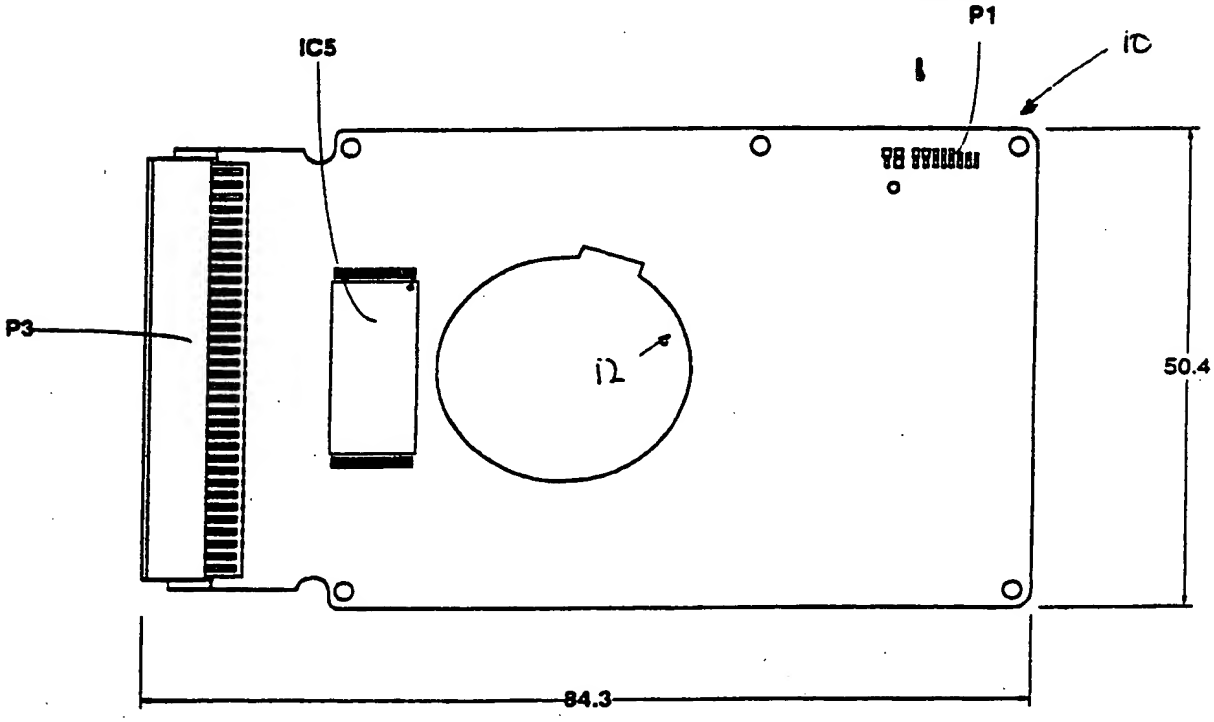
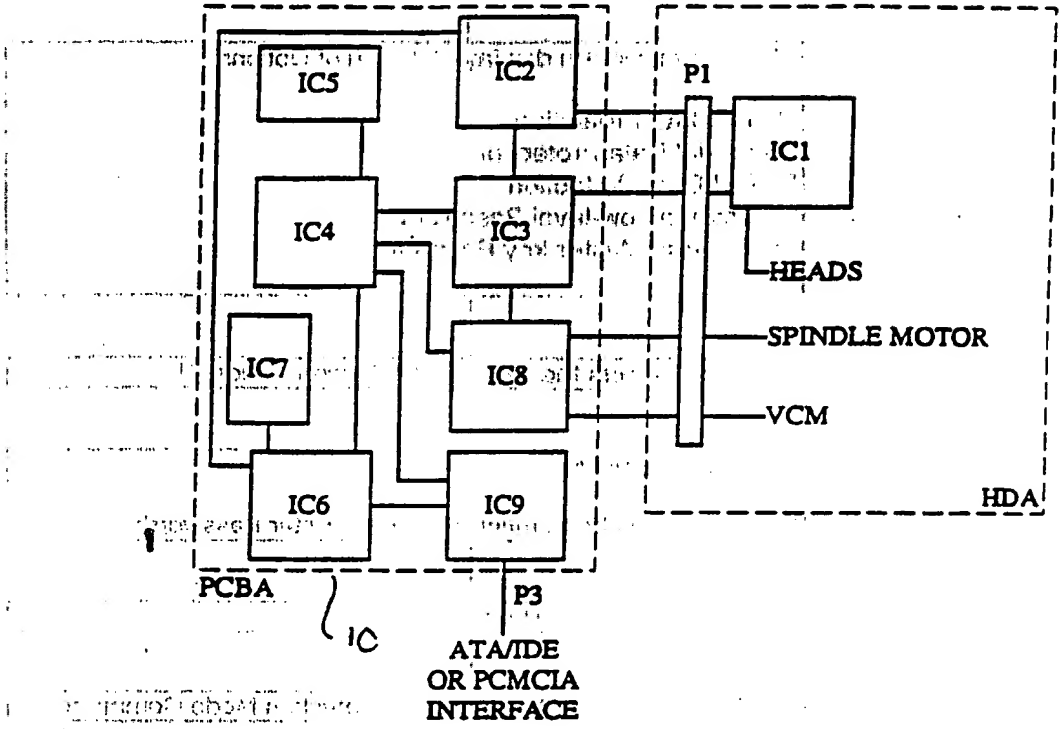


FIG. 2

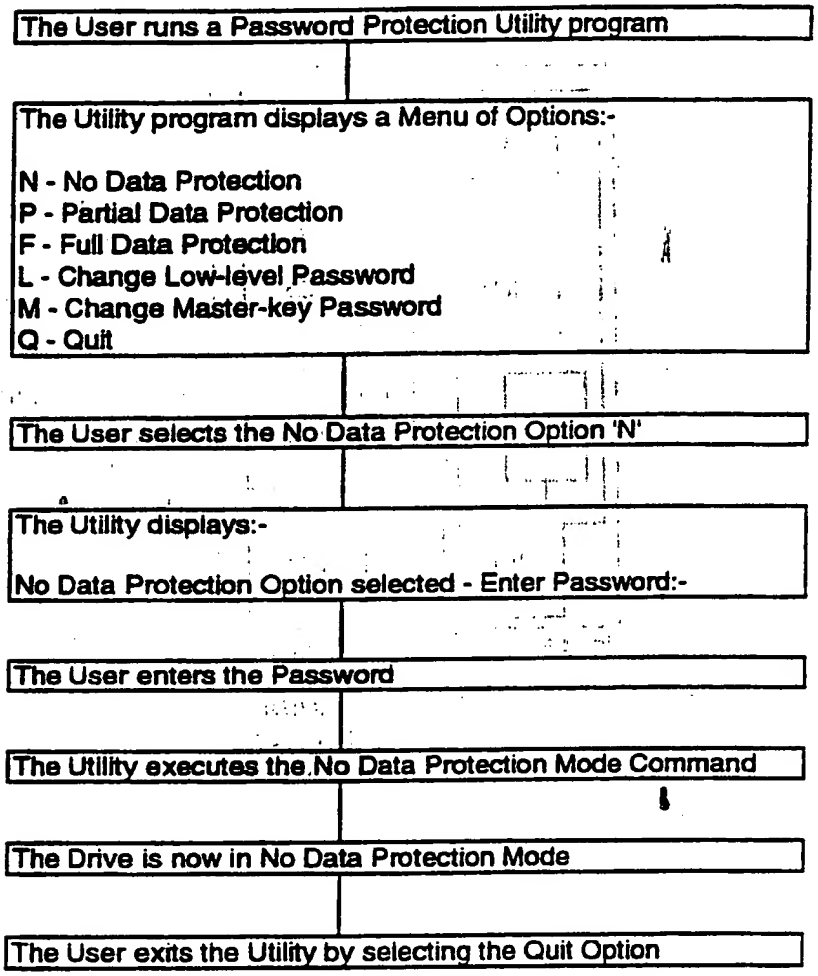


Block No	Function
IC1	Pre-amplifier
IC2	Data channel
IC3	Mixed signal ASIC
IC4	Micro-processor
IC5	Flash EEPROM
IC6	Interface
IC7	RAM
IC8	Motor/VCM driver/controller
IC9	Interface (PCMCIA)
P1	Elastomeric connector
P3	68 way connector

FIG.3

Password Protection Example

The User requires to set the hard disk into No Data Protection Mode



The other commands are executed in a similar fashion except that changing the Passwords Options would prompt the User for both the Old and the New Passwords.

FIG. 4

Password Protection Hard Drive Command Handling Sequence

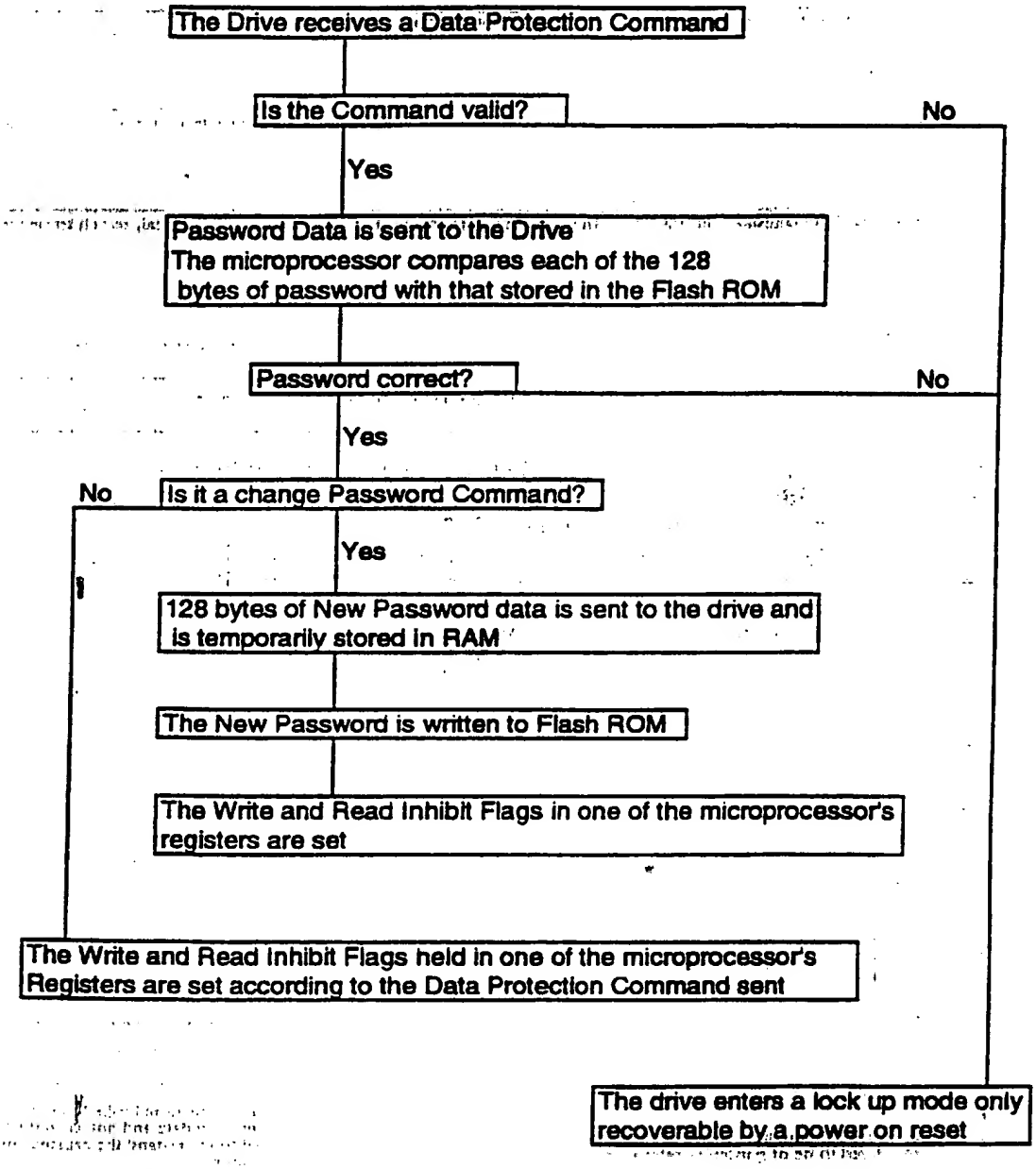


FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 94/02508

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US,A,4 864 542 (OSHIMA ET AL) 5 September 1989 see abstract; figures 1-3 see column 1, line 1 - column 2, line 61 see column 4, line 9 - column 5, line 66	1-5,7-15
Y	WO,A,90 00771 (VERWEYEN) 25 January 1990 see abstract; figures 1,5,7-9 see page 3, paragraph 3 see page 4, paragraph 4 see page 5, paragraph 1 see page 8, paragraph 4	1-5,7-15

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 February 1995	02.03.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 94/02508

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ELECTRONICS INTERNATIONAL, vol.55, no.3, February 1982, NEW YORK, US; pages 121 - 125 A.GUPTA ET AL '5V-Only EEPROM - Springboard for Autoprogrammable Systems' see the whole document	5
Y	EP,A,0 432 333 (IBM) 19 June 1991 see abstract; figure 2 see column 2, line 26 - column 3, line 35 see column 5, line 9 - line 51	8,10,11

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 94/02508

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-4864542	05-09-89	JP-A- 63225841	20-09-88
WO-A-9000771	25-01-90	DE-A- 3914239	11-01-90
		AU-A- 3848289	05-02-90
		EP-A,B 0428528	29-05-91
EP-A-0432333	19-06-91	AU-B- 636681	06-05-93
		JP-A- 3189821	19-08-91
		JP-B- 6038230	18-05-94
		US-A- 5265163	23-11-93